IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH APPLE ID KIERSTENNAPODANO@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	Case No. 24-SW-293

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT TO SEARCH AND SEIZE

I, Benjamin W. Grant, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), 2703(h)(5)(B) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cuptertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Homeland Security Investigations (HSI) Special Agent (SA) and have been since January 2017. I am currently assigned to the HSI Assistant Special Agent in Charge (ASAC), Memphis, Tennessee. I completed an intensive six-month academy at the Federal Law Enforcement Training Center, located in Glynco, Georgia, which included the Criminal Investigator Training Program and the HSI Special Agent Training Program. While attending the

BL

Federal Law Enforcement Training Center I received training in investigative areas including customs and immigration fraud, child sexual abuse material, human trafficking, narcotics smuggling, money laundering, bulk cash smuggling, the illegal exportation of weapons, munitions and high technology items, the illegal exportation of commodities, general smuggling, and alien smuggling. Before my employment with HSI, I earned a graduate degree from the University of Scranton and served in the U.S. Air Force.

STATUTORY VIOLATIONS

3. Based upon the information contained in this affidavit, I have probable cause to believe that information associated with Apple ID "KIERSTENNAPODANO@GMAIL.COM" (hereinafter SUSPECT ACCOUNT), is evidence, contraband, fruits, and instrumentalities of violations of federal law, namely 18 U.S.C. § 2252A, possession of child pornography, and 18 U.S.C. §§ 2422(b), coercion and enticement as more particularly described in Attachment B.

4. I make this affidavit in support of an application for a warrant to search SUSPECT ACCOUNT as described more fully in Attachment A, and to seize the items relating to violations of 18 U.S.C. § 2252A, and 18 U.S.C. §§ 2422(b) as more fully described in Attachment B. I make this affidavit to search SUSPECT ACCOUNT information to be disclosed by Apple Inc

5. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals participating in this investigation, including other law enforcement officers, my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a seizure and search warrant, it does not set forth each and every fact that I or others

have learned during this investigation.

DEFINITIONS

6. The below definitions apply to this Affidavit and Attachment B to this Affidavit.

7. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

8. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

9. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

10. This application seeks a warrant to search all responsive records and information under the control of Apple Inc., a provider subject to the jurisdiction of this court, regardless of where Apple has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Apple Inc.'s possession, custody, or control,

RG

regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

11. I am aware that many providers of digital services have staff members who work shifts other than traditional business hours. Such staff members may at times be responsible for compiling materials responsive to search warrants. Therefore, I request that this warrant be executable at any time of the day or night, as that may be more convenient for the responding party.

12. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

INVESTIGATION

13. On April 4, 2024, I learned information indicating Kiersten NAPODANO, a registered sex offender, was engaged in a sexual relationship with an identified minor victim (MV). The information I received also indicated that on April 4, 2024, NAPODANO and MV were possibly alone together in a vehicle. I coordinated with the Shelby County Sheriff's Office (SCSO) in an attempt to locate MV and NAPODANO.

14. Later the same day, SCSO encountered MV and NAPODANO in a Toyota sedan which was stopped after running a stop sign. MV, a 17-year-old with no driver license, was discovered operating the vehicle and NAPODANO was in the passenger seat. NAPODANO is a registered owner of the vehicle. I arrived on scene shortly thereafter.

15. I encountered MV at the scene and identified myself as a Special Agent with Homeland Security Investigations. MV provided the below statements in summary and not verbatim.

- MV stated the reason for being stopped was because MV did not fully stop at the stop sign and that they had no license.
- MV stated they were not in school because they did not want to go that day.
- MV stated the reason he was driving was because NAPODANO wanted to apply her makeup (SA note: NAPODANO did not appear to be wearing makeup).
- MV stated they were aware NAPODANO was a sex offender and that NAPODANO had disclosed that fact.
- MV stated they met NAPODANO approximately in December 2023, they talk and have each other's phone number.
- MV displayed NAPODANO's contact on their phone. It was saved as "Neida" a name MV said he gave her.
- MV stated he only calls and never texts NAPODANO or use social media with her.
- MV did not consent to a search of the "hidden images" album on their iPhone.
- MV stated NAPODANO knew he was a minor, 17 years old.
- MV denied having sexual contact with NAPODANO. MV stated they did not want to get NAPODANO in trouble and asked what was going to happen to her.

16. I also encountered NAPODANO at the scene and identified myself as a Special Agent with Homeland Security Investigations. I Mirandized her and asked if she was willing to speak with me. NAPODANO provided the below statements in summary and not verbatim.

- NAPODANO stated the driver was MV and identified them by their true first name.
- NAPODANO stated she does not have a license either but was giving him a ride.
- NAPODANO stated MV did not go to school that morning but that she was driving MV to school now (approximately 2pm) for a party or baby shower.

- NAPODANO was unable or unwilling to explain when and where she picked up MV on April 4, 2024.
- NAPODANO was unable or unwilling to provide a timeline of her day on April 4, 2024.
- NAPODANO stated she first met MV in January or February 2024 at an identified Memphis restaurant where they are employed.
- NAPODANO stated MV contacted her on April 4, 2024, via a Snapchat phone call and she picked him up.
- NAPODANO denied being under the influence of drugs or alcohol and stated the last time she used was four days prior.
- NAPODANO stated she took full responsibility for having MV drive unlicensed.
- NAPODANO denied having sexual contact with MV.
- NAPODANO denied consent to search her phone.
- NAPODANO stated nobody she knows, also knows MV.

17. MV was released from the scene to the custody of their mother. NAPODANO was charged by SCSO with violating the terms of her probation and transported to 201 Poplar.

18. On April 5, 2024, an identified source contacted me and stated they possessed SUSPECT DEVICE (said to be NAPODANO's Lenovo laptop.) The source stated NAPODANO wanted incriminating images to be removed from her devices and her iCloud account (SUSPECT ACCOUNT) to be wiped. They stated they wanted to turn it over because it contained evidence of NAPODANO being a predator. This information was corroborated by NAPODANO's first jail call. At approximately 7:20pm on the day of her arrest, she called an identified person. Their conversation included the following non-verbatim statements made by NAPODANO.

Approximately two minutes into her call, NAPODANO stated this is really, really important and I have to be limited on what I say. She stated her iCloud login name and password to the person and directed them to navigate to her Find My app, locate the option as if her device was stolen and erase all data. NAPODANO stated would you please do that; it's serious. Go in Find My and erase all data as fast as you can.

19. On April 5, 2024, I met with the identified source, and they turned over SUSPECT DEVICE (S/N: PF41EM0Z) and signed a property receipt. During this meeting, the source displayed sexual images on SUSPECT DEVICE to me. The images were displayed voluntarily and unprompted by me. I observed images that showed a male and female engaged in genital-genital penetration. The source stated the female is NAPODANO and the male is MV. I did not observed images with faces. The source stated the images they displayed and other information were linked to NAPODANO's Apple ID. The source also displayed NAPODANO's Apple ID on the device and I observed KIERSTENNAPODANO@GMAIL.COM (SUSPECT ACCOUNT).

20. Given the information referenced in paragraphs 13 through 16, I determined NAPODANO is a registered sex offender who was discovered alone with an identified minor in violation of her status. Given the fact pattern of this case and the information referenced in paragraphs 18 and 19, I determined the images I observed on SUSPECT DEVICE probably constitute child pornography as defined in 18 U.S.C. § 2256 and that the images are probably stored on and or associated with SUSPECT ACCOUNT.

INFORMATION REGARDING APPLE ID AND iCLOUD

21. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

22. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain

enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac.

23. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

24. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access

RL

most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

25. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

26. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

27. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

28. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored

on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

29. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

30. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Based on this investigation, I expect to find evidence of NAPODANO in a close continuing relationship with MV, including evidence of her sexual contact with MV. I expect to find evidence including but not limited to messages exchanged between NAPODANO and MV coordinating times or places to meet and visual depictions of her sexual contact with MV.

31. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date, and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier

RG

information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

32. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

33. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with potential additional unidentified minor victims. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of potential additional unidentified minor victims and instrumentalities of the crimes under investigation.

34. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the NAPODANO as an account user and provide evidence of her criminal violations.

CONCLUSION

35. I submit that there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A, and 18 U.S.C. §§ 2422(b) are located on

QL

SUSPECT ACCOUNT described in Attachment A. I, therefore, request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Respectfully submitted,

Benjamin W. Grant
Special Agent, HSI

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 41 by telephone, this 11th day of July, 2024.

s/Tu M. Pham

HON. TU M. PHAM
Chief United States Magistrate Judge